LILY HAY NEWMAN SECURITY 02.12.18 12:09 PM

NOW CRYPTOJACKING THREATENS CRITICAL INFRASTRUCTURE, TOO

Hijacking computers to mine cryptocurrency has branched out to dangerous places. HOTLITTLEPOTATO

The rise of cryptojacking—which co-opts your PC or mobile device to illicitly mine cryptocurrency when you visit an infected site—has fueled mining's increasing appeal. But as attackers have expanded their tools to slyly outsource the number of devices, processing power, and electricity powering their mining operations, they've moved beyond the browser in potentially dangerous ways.

On Thursday, the critical infrastructure security firm Radiflow announced that it had discovered cryptocurrency mining malware in the operational technology network (which does monitoring and control) of a water utility in Europe—the

control system.

Radiflow is still assessing the extent of the impact, but says that the attack had a “significant impact” on systems. The researchers note that the malware was built to run quietly in the background, using as much processing power as it could to mine the cryptocurrency Monero without overwhelming the system and creating obvious problems. The miner was also designed to detect and even disable security scanners and other defense tools that might flag it. Such a malware attack increases processor and network bandwidth usage, which can cause industrial control applications to hang, pause, and even crash—potentially degrading an operator’s ability to manage a plant.

″I’m aware of the danger of [malware miners] being on industrial control systems though I’ve never seen one in the wild,” says Marco Cardacci, a consultant for the firm RedTeam Security, which specializes in industrial control. “The major concern is that industrial control systems require high processor availability, and any impact to that can cause serious safety concerns.″

Low Key Mining

Radiflow CEO Ilan Barda says the company had no idea it might discover a malicious miner when it installed intrusion detection products on the utility’s network, particularly on its inner network, which wouldn’t usually be exposed to the internet. “In this case their internal network had some restricted access to the internet for remote monitoring, and all of a sudden we started to see some of the servers communicating with multiple external IP addresses,” Barda says. “I don’t think this was a targeted attack, the attackers were just trying to look for unused processing power that they could use for their benefit.”

Industrial plants may prove an enticing environment for malicious miners. Many don’t use a lot of processing power for baseline operations, but do draw a lot of electricity, making it relatively easy for mining malware to mask both its CPU and power consumption. And the inner networks of industrial control systems are known for running dated, unpatched software, since deploying new

platforms. These networks generally don't access the public internet, though, and firewalls, tight access controls, and air gaps often provide additional security.

Security specialists focused on industrial control, like the researchers at Radiflow, warn that the defenses of many systems still fall short, though.

"I for one have seen a lot of poorly configured networks that have claimed to be air gapped but weren't," RedTeam Security's Cardacci says. "I am by no means saying that air gaps don't exist, but misconfigurations occur often enough. I could definitely see the malware penetrating crucial controllers."

With so much fallow processing power, hackers looking to mine—often with automated scanning tools—will happily exploit flaws in an industrial control system's defenses if it means access to the CPUs. Technicians with an inside track may also yield to temptation; reports surfaced on Friday that a group of Russian scientists were recently arrested for allegedly using the supercomputer at a secret Russian research and nuclear warhead facility for Bitcoin mining.

"The cryptocurrency craze is just everywhere," says Jérôme Segura, lead malware intelligence analyst at the network defense firm Malwarebytes. "It's really changed the dynamic for a lot of different things. A large amount of the malware we've been tracking has recently turned to do some mining, either as one module or completely changing attention. Rather than stealing credentials or working as ransomware, it's doing mining."

Getting Serious

Though in-browser cryptojacking was a novel development toward the end of 2017, malicious mining malware itself isn't new. And more and more attacks are cropping up all the time. This weekend, for example, attackers compromised the popular web plugin Browsealoud, allowing them to steal mining power from users on thousands of mainstream websites, including those of United States federal courts system and the United Kingdom's National Health Service.

individual devices like PCs or smartphones. But as the value of cryptocurrency has ballooned, the sophistication of attacks has grown in kind.

Radiflow's Barda says that the mining malware infecting the water treatment plant, for instance, was designed to spread internally, moving laterally from the internet-connected remote monitoring server to others that weren't meant to be exposed. "It just needs to find one weak spot even on a temporary basis and it will find the way to expand," Barda says.

Observers say it's too soon to know for sure how widespread cryptojacking will become, especially given the volatility of cryptocurrency values. But they see malicious mining cropping up in critical infrastructure as a troubling sign. While cryptojacking malware isn't designed to pose an existential threat—in the same way a parasite doesn't want to kill its host—it still wears on and degrades processors over time. Recklessly aggressive mining malware has even been known to cause physical damage to infected devices like smartphones.

It also seems at least possible that an attacker with goals more sinister than a quick financial gain could use mining malware to cause physical destruction to critical infrastructure controllers—a class of rare but burgeoning attacks.

"We've seen this technique with ransomware like NotPetya where it's been used as a decoy for a more dangerous attack," Segura says. "Mining malware could be used in the same way to look financially motivated, but in fact the goal was to trigger something like the physical damage we saw with Stuxnet. If you run miners at 100 percent you can cause damage."

Such a calamitous attack remains hypothetical, and might not be practical. But experts urge industrial control plants to consistently audit and improve their security, and ensure that they've truly siloed internal networks, so there are no misconfigurations or flaws that attackers can exploit to gain access.

"Many of these systems are not hardened and are not patched with the latest

and other malware threats is much more problematic in industrial control system networks," says Jonathan Pollet, the founder of Red Tiger Security,

plants and natural gas utilities. "I hope this helps create a sense of urgency."

Cryptojack Attacks

- Cryptojacking has come a long way since the fall, when it was a much smaller-scale operation
- Even its more aggressive implementations didn't match the critical infrastructure concerns we're seeing today
- And malware used to pull off physical, real-world attacks can do some serious large-scale damage

VIEW COMMENTS

MORE SECURITY

Equifax Found 2.4 Million More People Hit By Its Breach

LILY HAY NEWMAN

PROPAGANDA

Facebook Doesn't Know How Many Followed Russians on Instagram

ISSIE LAPOWSKY

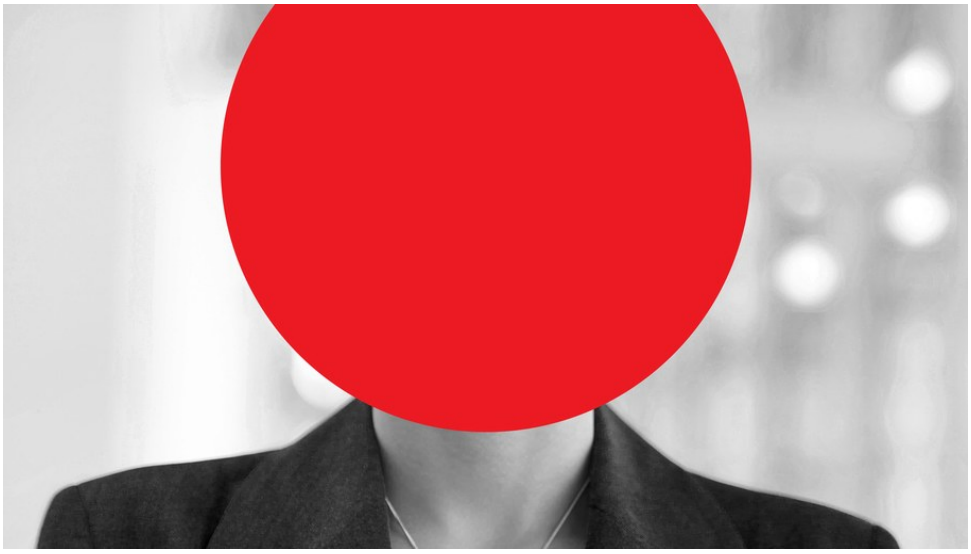
DAVID NEWMAN

TWO-FACTOR

Chrome Lets Hackers Phish Even 'Unphishable' Yubikey Users

ANDY GREENBERG

INTERNET



PRIVACY

How to Turn Off Facebook's Face Recognition Features

LILY HAY NEWMAN

GET OUR NEWSLETTER

WIRED's biggest stories delivered to your inbox.

Enter your email

SUBMIT

FOLLOW US ON YOUTUBE

FOLLOW

SUBSCRIBE	ADVERTISE
SITE MAP	PRESS CENTER
FAQ	ACCESSIBILITY HELP
CUSTOMER CARE	CONTACT US
SECUREDROP	T-SHIRT COLLECTION
NEWSLETTER	WIRED STAFF
JOBS	RSS